ARMY RESEARCH LABORATORY

A Survey of Visualization Tools Assessed for Anomaly-Based Intrusion Detection Analysis

by Renée E. Etoty and Robert F. Erbacher

ARL-TR-6891 **April 2014**

NOTICES

Disclaimers

The findings in this report are not to be construed as an official Department of the Army position unless so designated by other authorized documents.

Citation of manufacturer's or trade names does not constitute an official endorsement or approval of the use thereof.

Destroy this report when it is no longer needed. Do not return it to the originator.

Army Research Laboratory
Adelphi, MD 20783-1197

ARL-TR-6891 **April 2014**

A Survey of Visualization Tools Assessed for Anomaly-Based Intrusion Detection Analysis

Renée E. Etoty and Robert F. Erbacher
Computational and Information Sciences Directorate, ARL

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED (From - To)
April 2014	Final	01/2013 to 09/2013

4. TITLE AND SUBTITLE
A Survey of Visualization Tools Assessed for Anomaly-Based Intrusion Detection Analysis

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Renée E. Etoty and Robert F. Erbacher

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
U.S. Army Research Laboratory
ATTN: RDRL-CIN-D
2800 Powder Mill Road
Adelphi, MD 20783-1197

8. PERFORMING ORGANIZATION REPORT NUMBER
ARL-TR-6891

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT
Security visualization remains relatively an immature term. The idea of security visualization is the need for novel techniques that are fine-tuned for aiding cyber security analysts in distinguishing benign and malicious data. Intrusion Detection Systems (IDS) aim to do just that and the focus is more on the detection capability and not on presentation to the end user. For example, Snort logs a variety of information to a flat text file that requires additional parsing. The shortcoming of IDS is that no satisfactory solution to using visualization as an aid to intrusion detection (ID) has been developed and deployed. In particular, this report chooses to focus on the survey of current visualization tools that can enhance an IDS becoming more deployable. From this assessment, we provide suggestions of visualization tool compatibilities that best meet the needs of the anomaly-based intrusion detection analysis.

15. SUBJECT TERMS
visualization tools, anomaly-based intrusion detection tools

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Renée E. Etoty
Unclassified	Unclassified	Unclassified	UU	50	19b. TELEPHONE NUMBER (*Include area code*) 301-394-1835

Standard Form 298 (Rev. 8/98)
Prescribed by ANSI Std. Z39.18

Contents

List of Figures

List of Tables

1. Introduction

1.1 Overview

Visualization in general is a particular method of interest being explored to aid the end users' environment to enable more analysis that is effective. It is also used to increase the overall performance in user friendliness and interaction with the device. This report presents a technology assessment of the current available visualization tools that can be used to enhance accuracy, communication, and performance of the analyst's process of identifying cyber attacks with anomaly-based Intrusion Detection Systems (IDS). The goal of this assessment is to provide a list of visualization tools for the developers that may integrate in ensemble with other techniques making the overall IDS system more deployable.

There are well over one hundred visualization tools currently available. We used the following metrics to select which tools would be most applicable to the cyber security domain:

- Relevance to network security
- Breadth of visual techniques
- Ease-of-use
- Ability to answer the concerns of end users

This resulted in a final list of 59 visualization tools to analyze. We reviewed and grouped the selected 59 visualization tools into the following categories of visualization needs for analyst tasks:

- Predevelopment
- Monitoring
- Analysis
- Response
- Future Development

The analysis recommends and proposes the use of visualization tools that best meet the requirements and specifications of the end users within the five categories. Here the end users are a targeted audience composed of decision makers, analysts, other end users, and a special interest group at the U.S. Army Research Laboratory (ARL).

Anyone involved in the various aspects of cyber security especially those that are decision driven such as analysts tasks should be interested in our findings. Use of this visualization tools

assessment is necessary to improve the user interface or user environment that the analysts interact with to detect and prevent attacks on cyber networks. Having this information enables better situational awareness for the entire network security community and knowledge superiority in the cyber domain. Furthermore, this assessment aids network and communication sciences by developing an ensemble of techniques that allow the user interface to provide better information assurance.

1.2 Intrusion Detection Systems (IDS)

IDS aim at detecting attacks against computer systems and networks or, in general, against information systems (*1*). It acquires knowledge about an information system in order to perform analysis on its security status. It is important to note that there are two general types of IDS: knowledge-based and behavior-based. Knowledge-based IDS is often referred to as "misuse detection" (*2, 3*) or detection by appearance (*4*). A knowledge-based IDS is designed to collect network information and sift through the collected data for evidence of exploitation, command, and control. In the same fashion, behavior-based IDS is also known as anomaly detection (*4*) or detection by behavior and its focus is on creating a model of usual behavior for the information system being monitored while observing any deviation from the model for further investigation.

Some other IDS are signature-based, host-based, network-based, and graph-based. Signature-based IDS decides in advance what type of behavior is undesirable according to the use of known set behaviors and detected intrusions (*5*). Host-based was the first IDS ever designed to audit information provided by a mainframe (*6*). It performed its audit locally or on separate machines (*6*). A shift in computing from mainframe environments to distributed workstation networks was the cause for seeking better IDSs (*2*). Out of this came the Distributed IDS (DIDS) that is the hybrid approach to using both network-based and host-based intrusion detection (ID) tools for a multihost environment (*9*). Network-based IDS is the design philosophy of mining network traffic at the network level, auditing packet information, and logging any suspicious packets, connections, or sessions into a special log file with extended information (*8*). Graph-based IDS (GrIDS) is designed to detect large-scale automated attacks on network systems. It puts together reports of incidents and network traffic into graphs, and is able to aggregate those graphs into simpler forms at higher levels of the hierarchy (*9*).

The known existing issues with anomaly-based IDS include the tendency to consume data processing resources, the possibility of an attacker teaching the system that illegitimate activities are ordinary or regular (*5*). Similar known IDS issues (*1, 11*) contribute to the limit of employed anomaly-based IDS for the past 25 years. The idea for IDS was first introduced in 1987 by Dorothy Denning (*12*) and many still focus on the development of deployable anomaly-based IDS. With this mission, comes the question of how to interpret the information outputted to the end user by the anomaly-based IDS? Therefore, one method to address this mission is to use visualization and or visualization techniques.

The goal of an IDS is to properly characterize attack behaviors to positively identify all true attacks without falsely identifying nonattacks (*13*) meaning that the true positives are increased while the false positive rate is decreased. Therefore, it is best to consider both views of an attack situation on a network system where its data may be affected. From an attack victim's view, the following are the major concerns:

- Where and when did the intrusion originate?
- What happened?
- How and why did the intrusion happen?
- Who is affected and how?
- Who is the intruder?

From the attacker's view, the following are major concerns:

- What is my objective?
- What vulnerabilities exist in the target system?
- What damage or other consequences are likely?
- What exploit scripts or other attack tools are available?
- What is my risk of exposure?

1.3 Visualization

The design of visualization techniques for the exploration, analysis, and situational awareness of network events has become a significant focus of researchers as they attempt to deal with the sheer volume and complexity of the data (*13*). This has resulted in two cognitive task analysis (*15, 16*) examining the needs and requirements of network analysts and managers. In reference 15, the study used event-related functional magnetic resonance imaging (fMRI) to study the pattern of activation during four distinct stages in the performance of the Wisconsin Card Sorting Task (WCST). Ellis et al. (*16*) conducted an explorative analysis on user evaluation studies that use information visualization. They found that an empirical evaluation of visualizations alone is methodologically unsound because of its generative nature. Their results do show that empirical evaluations used in conjunction with reasoned justification leads to a more reliable validation of the visualization. This direction of research has resulted in the development of enumerable visualization techniques. The entire community, Visualization Security (VizSec) (*17*) has been formed around the research task of visually analyzing and monitoring network data, which is usually reviewed at their yearly conference.

Visualization has a history of being nondeployable, ineffective, and obfuscating especially for the analyst, our end user. The overall goal with using visualization tools and techniques is to

integrate them with interaction techniques effective for large-scale databases to analyze the data and identify sophisticated attacks within the arriving data (*18*). We plan to explore current computer-graphics interaction techniques via input displays. Furthermore, visualization is to be used in ensemble with other techniques that will reduce the effect of having the false positive rates increasing faster than the true positive rates that will in turn make anomaly detection more deployable (*19*).

Visualization for ID can help a security administrator to recognize abnormal behavior in an intuitional manner. Visualization of ID can enable better analysis and response because an intrusion is recognized intuitionally. Therefore, it can overcome alert flooding. Most ID methods with visualization are anomaly-based detection methods and visualize audit data rather than the alert itself (*20*). The host-based visualization method for ID is to learn normal states of commands or programs that is achieved by the user and compares audit data with profiles for visualization.

Network-based visualization method used for ID expresses the source address, destination address and port number, and so forth, of the network's packets by visual graph (*20, 21*). They detect an intrusion when an attack differs from graph characteristic with normal state and extract diagnostic features of attack for embodying anomaly detection. However, these methods do not visualize alerts but visualize audit data. They are however useful for detecting attacks that emit much traffic such as distributed denial-of-service (DDoS) attack (*22*). This method does not offer clear features for attacks that emit little traffic (*23*).

The goal of this report is to provide a reliable list of visualization tools that will aid in the goals of implementing the expansion of the anomaly-based IDS framework through user interface characteristics that when implemented in ensemble with other detection techniques will do the following (*3*): provide prioritized information distinguishable from noise in the anomaly-based IDS user interface, increase situational awareness as a result, and has ease of use for the end user. Hence, it is with the efforts of aiding decision makers that this paper assesses current visualization tools that improve the decision-making process enabling analysts and any end user to make decisions and choose better actions (*24*).

2. Desired Visualization Needs for Analysts Tasks

Understanding the problem requires understanding the perspective of the developers and the users. It is important to first acknowledge the audience who will be using the displays, environment, or product that will employ the visualization tools. This particular audience by inferred assumption includes the analysts, the decision makers, and any other end users. An immediate focus is on the interviewed analysts, decision makers, and end users that provide the requirements and specifications for their needed environment. With this in mind, it was fitting to

first obtain their perspective on what components are important and valuable to their interaction and understanding of data with the final user interface. We used their initial responses from a user study conducted in a brainstorming session consisting of network analysts, network managers, security researchers, and visualization researchers at Pacific Northwest National Laboratory* (PNNL) and with the United States Air Force Research Laboratory† (AFRL) (*24*). Their documented responses enabled a focused literature review to seek out current visualization tools that currently exist and would meet most of the requirements for this audience. The assessed visualization tools include applications, software, API's, programming languages, and specific environments. The intent and hopes for a wide variety in tool type is for more options in ensemble with other techniques that will make the user interface deployable. Collections of concerns from the end-users perspective (refer to reference 24) include:

- Visualize abstract concepts more effectively.
- Have clear focus on either mission impact or system impact.
- How to visualize amount of damage?
- How to visualize the identified attacks and attackers?
- How to visualize the characterization of attacks and attackers?
- How to visually identify a legitimate user?
- How to visually identify any abnormalities?
- How to visually identify a malicious actor?
- How to visually identify a compromised system?
- How to visualize an intended target of an attack through trace back?

*902 Battelle Blvd, Richland, WA 99354.

†Wright-Patterson Air Force Base, OH.

These questions cover the breath of end-users' initial brainstormed concerns session from reference 24:

- What assumptions is the software making?
- Visualization must identify the impacts of the breaches. How will network operation be affected?
- The software must address what is interesting to look at. This depends on viewer's perspective.
- What is most helpful to the user will depend on that particular user, their particular job, and their particular goals.
- The visualization must understand the various perspectives of different users.
- Templates will aid in identifying what is normal.
- Concepts for what is appropriate for templates, how they can most effectively be used and interpreted correctly.
- Need a communication capability to monitor the resolution of an attack and verify that the resolution plan is used.
- There should be a "network of trust" built into the visualization.
- How a timeline is used for ordering of events and actions is critical.
- The visualization should be able to determine what protocol the attack uses—common, unusual, or uncommon protocols.
- The visualization should organize data in a meaningful way. Usually, the 3-D viewpoint factors in time.
- Need to incorporate a communication medium within the visualization tool like a whiteboard or sticky notes to share data.
- It is important for the visualization to know what triggered the incident whether specific or generic.
- The visualization will need to know some basic information to what is happening outside the system to better understand and handle situational awareness.
- It is important to have a geo-location integrated into the visualization environment.

- Three things should be incorporated into the visualization organization:
    - Representation of generalized attack path
    - Representation including all nodes and routers
    - Representation of a timeline of events

The ID tasks and visualization needs process model developed by Komlodi et al. (*25*) is a clear indicator and starting point for making tools to meet analysts requirements. We took their model (see table 1) and combined it with the results from the PNNL and AFRL brainstorming session with expert analysts to obtain a more inclusive list of visualization needs required for analyst's tasks. Table 1 for the original model and table 2 the updated model with combined needs from the PNNL and AFRL brainstorm session.

Table 1. ID tasks and visualization needs table (*25*).

Phase	Analyst Tasks	Visualization Needs
Monitoring	• Monitoring all attack alerts • Identifying potentially suspicious alerts	• An overview of the alert data • Simple displays • Support for pattern and anomaly recognition • Flexibility • Speed of processing
Analysis	• Analyzing alert data • Analyzing other related data • Diagnosing attack	• Multiple views, zoom, drill down, focus + context solutions • Correlation between displays, linked views • Filtering and data selection
Response	• Responding to attack • Documenting and reporting attack • Updating IDS	• Suggestion for response action • Incident reporting • Annotation/feedback to facilitate future analysis • Saving views • Historical display • Reporting data transfer

Table 2. Updated ID tasks and visualization needs table.

Phase	Analyst Tasks	Visualization Needs
Pre-Development	❖ Need for systems analysis and design ❖ Incorporate human-computer interactions (HCI) ❖ Forefront approach of moving away from organizational and system needs to human needs	• Incorporate more effective and abstract concepts to visualize • Build "network of trust" into the visualization system • Incorporate a communication medium to share data • Integrate geo-location into environment ❖ Incorporate human processing capabilities to analyze patterns and images
Monitoring	• Monitoring all attack alerts • Identifying potentially suspicious alerts	• An overview of the alert data • Simple displays • Support for pattern and anomaly recognition • Flexibility • Speed of processing o Identify abnormalities o Identify impacts of breaches o Understand user perspective o Use timeline to order events and actions
Analysis	• Analyzing alert data • Analyzing other related data • Diagnosing attack	• Multiple views, zoom, drill down, focus+ context solutions • Correlation between displays and linked views • Filtering and data selection o Have clear focus on either mission impact versus system impact o Visualize characterization of attacks and attacker o Visualize identity of legitimate user o Switch between viewer perspectives to address what is interesting to look at o Usage of templates o Provide multi-dimensions beyond 2-D o Representation for generalized attack path o Representation that includes all nodes and routers o Representation of a particular timeline of events
Response	• Responding to attack • Documenting and reporting attack • Updating Intrusion Detection System (IDS)	• Suggestion for response action • Incident reporting • Annotation/feedback to facilitate future analysis • Saving views • Historical display • Reporting data transfer o Visualize identified attacks and attackers o Visualize malicious actor o Visualize compromised systems o Visualize an intended attack through trace back
Future Development	❖ Improving organizational processes for the entire analysis system	❖ Allow others to view current attack ❖ Integrate real-time (dynamic) animation ❖ Connect global resources visually ❖ Increase collaboration capabilities ❖ Incorporate data and report sharing on various networks

Key	
•	Visualization Needs According to Komlodi et al. (*25*)
o	Visualization Needs According to PNNL
❖	Added Visualization Needs

3. Methodology

Preamble

Step one is to understand the problem from the right perspectives. We are purposely choosing to focus on the user's (analysts) perspective as the right perspective for this survey.

Step two is conduct literature review on existing visualization tools and techniques that have capabilities to meet the visualization needs of the analysts according to their requirements list.

Step three is pinpointing the types of visualization tools that could aid analysts' tasks in anomaly-based IDS.

Step four is to analyze the actual visualization tools' capabilities and evaluate their level of potential to meet the requirements and specifications of the end users.

Step five is to do cross referencing with the capabilities of the final selected visualization tools to that of the visualization tools needed to perform analysts tasks at the five different phases.

Step six is to consider other factors that influence the decision of using a visualization tool.

Step seven is to analyze and make sense of the assessment.

Each step is further detailed in the following:

1. Understand the needs, concerns, and requirements from the perspective of the end users. This will provide a clearer direction for what types of visualization tools to research.
2. Conduct a literature review on visualization tools with high potential of meeting the requirements and specifications of the end users.
3. Focus literature review to include only the following types of visualization tools:
    - Visual programming languages
    - Visual software packages/kits
    - Visual libraries
    - Visual and graphical data representations
    - Innovative visual tools that can be applied to the network security domain
4. Remove the visualization tools that had minimal applicability in the network security domain.

5. Cross-reference the final list of visualization tools to the identified visualization needs for analysts task organized into the five categories that represent the different phases of analysts' tasks.
6. Consider other basic factors that may influence one's decision about using a given visualization tool. We look at the following factors:
    - Cost of visualization tool
    - Breath of environments used on platforms
    - Programming languages used—if any
    - Integration capability
7. Analyze assessment and determine its meaning.

4. Most Important Features for Visualizing Network Data

A network consists of links and nodes. It is important to first know the data. Spatial information and data statistics may be associated with these links and nodes. Our goal is to understand the data and not the networks themselves. Looking at the structure and connectivity of a graph provides valuable relationships and significant importance. In such relationships, we care about understanding the data associated with links and nodes. The link-node relationships are further examined on visual displays. Thus, the network shown on the visual display is determined by the parameters of the visual display. Meaning the values selected for each parameter of the visual display control the characteristics that generate the final network seen on the visual display. We call the parameter for the visual network display "features of interest." According to Becker et al. (*21*) some of the most common features of interest include:

- Statistic
- Levels
- Geography/Topology
- Time
- Aggregation
- Size
- Color

Setting the values of each parameter produces many combinations of parameters. The task becomes identifying which combinations of parameters lead to the most valuable and interpretable displays. The easiest way to allow for this is by allowing the analyst or end user to manipulate directly the values of parameters for the visual network display. This process is called direct manipulation. Direct manipulation enables at least the following parameters:

- Identification
- Linkmap Parameter Controls
- Matrix Display Parameter Controls
- Nodemap Parameter Controls
- Animation
- Zooming
- Physical Attributes (color, size, shape, etc.)

5. Visualization Tools Breakdown

The literature review resulted in 59 visualization tools that their capabilities are applicable to aiding network security analysts' tasks. We purposely chose to focus on capabilities from each tool that would specifically aid network security tasks done by the analysts, our end users. These tools have been regrouped into similar types such as Cooperative Association for Internet Data Analysis (CAIDA) tools (*26*), visualization programming language tools, visualization software packages/kits, visualization libraries, graphical data representation tools, and tools that we deem as a novel or creative approach for solving cyber network domain are lumped into the innovative tools. A brief description of each group and the sub-list of visualization tools are provided here. Figure 1 is an overview of the assessed visualization tools broken down into groups.

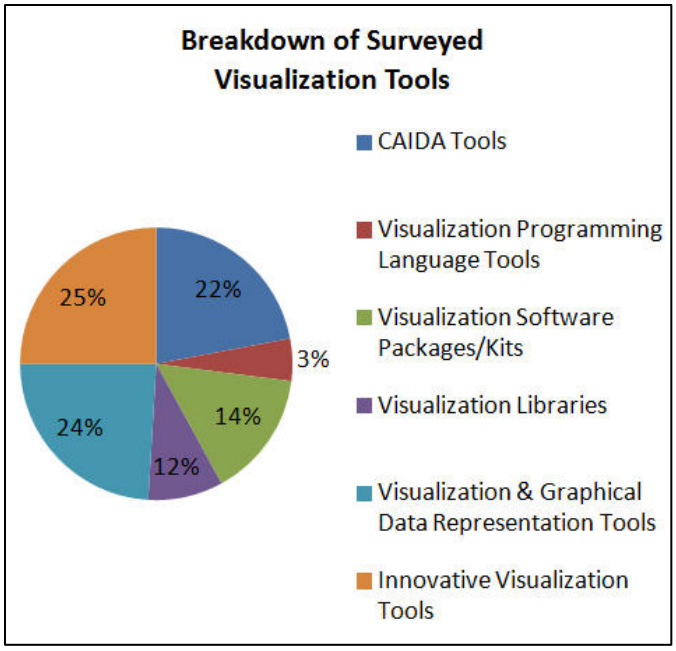

Figure 1. Breakdown of assessed visulation tools.

5.1 CIADA Tools

The CIADA is a collaborative undertaking among organizations in the commercial, government, and research sectors aimed at promoting greater cooperation in the engineering and maintenance of a robust, scalable global internet infrastructure (*27*). CAIDA provides macroscopic insights into internet infrastructure by looking at behavior, usage, and evolution. They foster a collaborative environment in which data can be acquired, analyzed, and shared when appropriate (*27*). Their goal is to improve the integrity of the internet science field as well as inform science, technology, and communications about public policies. They created tools to attend to routing, addressing, topology, workload characterization, network security, Domain Name System (DNS), performance, and trends. Out of all their available tools, thirteen of them are most applicable to aiding network security analysts' tasks. They are AutoFocus, Beluga, Cichild, Cuttlefish, FlowScan, GeoPlot, GTrace, MapNet, Otter, Plankton, PlotPaths, Real Traffic Grabber (RTG), and Walrus. The CAIDA tools account for 13/59=22% of the total visualization tools surveyed for network security analysts' tasks. Table 3 highlights the strengths and weaknesses of each visualization tool in this group.

Table 3. CAIDA tools capabilities.

CAIDA Tools Capabilities			
Name	**Web Site (all accessed 1/29/2014)**	**Strengths**	**Weaknesses**
AutoFocus	http://www.caida.org/tools/measurement/autofocus/	Produce reports and plots for various time periods ranging from weeks to half hour intervals; drill-down capability.	Few monitoring capabilities; no analysis capabilities; and one response capability.
Beluga	http://www.caida.org/tools/measurement/beluga/gallery/	Interactive frontend to trace-route data.	Few monitoring capabilities; no analysis nor response capabilities.
Cichlid	http://www.isoc.org/inet2000/cdproceedings/1d/1d_3.htm	Collects large amounts of data through Transmission Control Protocol (TCP) connections; does animation of bar charts and vertex and edge graphs; can be used as a server; 3-D and zoom views+.	Few analysis capabilities; no monitoring nor response capabilities.
Cuttlefish	http://www.caida.org/tools/visualization/cuttlefish/witty-hosts.xml	Geographical maps; color coded data; moving boundary line; optional color legend; single image; collection of related images; animated Graphics Interchange Format (GIF).	One monitoring capability; no analysis nor response capabilities.
FlowScan	https://www.usenix.org/legacy/events/lisa00/full_papers/plonka/plonka_html/	Analyzes and reports on NetFlow data; examines data and maintains counters.	Few analysis and response capabilities; no monitoring capabilities.
GeoPlot	http://www.caida.org/tools/visualization/geoplot/	Plots a set of nodes and a set of lines that connect these nodes on an image specified by the user.	Few analysis capabilities; no monitoring nor response capabilities
GTrace	http://www.caida.org/tools/visualization/gtrace/snapshots/	Flexible to support additional databases; heuristics to map Internet Protocol (IP) addresses to physical location and maps.	One monitoring and one analysis capability; no response capabilities.
MapNet	http://www.caida.org/publications/visualizations/	Ability to control complexity; flexibility in presentation; subset data in real-time; and view network with or without background map.	One monitoring and one analysis capability; no response capabilities.

Table 3. CAIDA tools capabilities (continued).

CAIDA Tools Capabilities			
Name	**Web Site (all accessed 01/29/2014)**	**Strengths**	**Weaknesses**
Plankton	http://www.caida.org/tools/visualization/plankton/	Provides topological or geographical display; toggle, zoom and pan; move single node or sub-tree; coloring; and time sequence animation.	One monitoring and one analysis capability; no response capabilities.
Otter	http://www.caida.org/tools/visualization/otter/otter_plots/	Visualize node, link, or path; high memory usage for large data sets; geographical or topological placement; modification of the display via zoom, focus, and other graph layout options.	One monitoring capability; no analysis nor response capabilities.
PlotPaths	http://www.caida.org/tools/visualization/plotpaths/plotpaths_shots.xml	Calculate node dept, create rows and columns; prevent vertical link overlap; assign x and y coordinates to nodes; and arrange nodes horizontally.	One analysis capability; no monitoring nor response capabilities.
RTG	http://www.caida.org/tools/measurement/rtg/	Runs as a daemon; written in C; multithreaded; use of relational database; and polls at sub-one minute intervals.	Windows platform is not supported; one monitoring capability; no analysis nor response capabilities.
Walrus	http://www.bcliving.ca/garden/what-does-the-internet-look-like	Indicates user's page activities; accumulates user accesses over time to identify Web pages that are visited more often; allows direct navigation.	Few monitoring capabilities; one analysis capability; no response capabilities.

5.2 Visualization Programming Language Tools

Visual programming language (VPL) tools are those that in computing are considered to allow the user to create programs by manipulating program elements graphically instead of textually (*28*). VPL provides this programming through visual expressions and spatial arrangements of text or graphic symbols. The VPL tools accounted for in this survey includes ClojureAtlas, GINY, and Processing JS. These VPL tools make up 2/59=3.0% of the total visualization tools surveyed for the network security analysts' tasks. Table 4 highlights the strengths and weaknesses of each visualization tool in this group.

Table 4. Visualization programming language tools' capabilities.

Visualization Programming Language Tools' Capabilities			
Name	**Web Site (all accessed 01/29/2014)**	**Strengths**	**Weaknesses**
ClojureAtlas	http://fsteeg.com/2012/02/26 /visualize-clojure-code-in-eclipse-with-dot-and-zest/	Efficient and robust infrastructure for multithreaded programming; compiles directly to JVM and remains completely dynamic.	No monitoring nor analysis capabilities; one response capability.
Processing JS	http://processingjs.org/	Does typography, math, shapes, structures, images, and rendering; has various transformations, data types, input types, controls, input and output formats; has light and camera settings; creates environment.	No response capabilities.

5.3 Visual Software Packages and Kits

Visualization software usually incorporates a range of computer graphic products used to create graphical display or interfaces for software applications. The visualization software tools accounted for in this survey includes Complex System SCILAB Toolbox, GraphViz, Igraph, NetDraw, Network Workbench, OpenDX, Prefuse, Sci² Tool, and Visualization Toolkit (VTK). They make up 8/59=13.55% of the total visualization tools surveyed for the network analysts' tasks. Table 5 highlights the strengths and weaknesses of each visualization tool in this group.

Table 5. Visualization software packages and kits' capabilities.

Visualization Software Packages and Kits' Capabilities			
Name	**Web Sites (all accessed 01/29/2014**	**Strengths**	**Weaknesses**
Complex Systems SCILAB Tool	http://www.randomfactory.com/openastro/osx/scilab-info.html	Measures graph parameters	Academic Free License (AFL); works on UNIX and Windows; programming language is MATLAB; no analysis or response capabilities.
GraphViz	http://kurata21.bio.kyutech.ac.jp/grid/grid_layout.htm	Has features for concrete diagrams, such as options for colors, fonts, tabular node layouts, line styles, hyperlinks, roll and custom shapes; works on all major platforms.	Eclipse Public License (EPL) v1.0; one monitoring capability; no analysis nor response capabilities.
NetDraw	http://electricosas.blogspot.com/2011/10/netdraw-y-laku-dr-ing-hans-detlef.html	Generate and manipulate graphs, easy to install and use, fully integrated with Ucinet, integrates with Pajek, has command-line language to help automate procedures.	Windows platform only, performs basic analysis, has been used for social networks only, system documentation not fully developed; no response capabilities.
Network Workbench	http://scimaps.org/atlas/part3.html	Provides means to carry out network analysis, modeling, and visualization projects in own fields; and provides shared resource environment.	No monitoring capabilities; few analysis capabilities.
OpenDX	http://www.opendx.org or http://vlsicad.eecs.umich.edu/BK/Slots/cache/www.opendx.org/index2.php	Visualization for scientific, engineering, and analytical data; open source; can handle overlapping grids with ease.	Graphical User Interface (GUI) is not really compatible for network data in the cyber security sense; no monitoring, analysis, or response capabilities.
Prefuse	http://weka.wikispaces.com/Explorer+tree+visualization+plugins	Dynamic queries; animation support; table, graph, and tree data structure support; panning and zooming; flexibility for multiple views.	Ease-of-use is medium to difficult; no analysis or response capabilities.
Sci² Tool	http://www.vivoweb.org	Supports temporal, geospatial, topical, and network analysis; does visualization of datasets at the micro (individual), meso (local), and macro (global) levels.	Made for sciences in general; no monitoring capabilities.
Visualization Toolkit (VTK)	http://www.vtk.org/	Does scalar, vector, tensor, texture, and volumetric methods; advanced modeling; implicit modeling, polygon reduction, mesh smoothing, cutting, contouring, and triangulation.	Ease-of-use is medium to difficult; no response capabilities.

5.4 Visualization Library Tools

Visualization libraries are an extension of visualization software and usually come in packages or toolkits. The visualization library tools accounted for in this survey includes Impure (now Quadrigram), InfoVis CyberInfrastructure, Jgraph, JUNG, and the Visualization library. They make up 7/59=11.86% of the total visualization tools surveyed for the network analysts' tasks. Table 6 highlights the strengths and weaknesses of each visualization tool in this group.

Table 6. Visualization library tools' capabilities.

Visualization Library Tools' Capabilities			
Name	**Web Sites (accessed 01/29/2014)**	**Strengths**	**Weaknesses**
Impure now Quuadrigram	http://www.quadrigram.com/in_action	High interoperability, publish publically or share privately, geo-data, quadrification, and stack flow.	Ease of use is more difficult for a nonprogrammer, a nonengineer, or anyone unfamiliar to data analysis.
InfoVis Cyber-Infrastructure	http://iv.slis.indiana.edu/sw/	Integration of algorithms as plug-ins, completely open source, and allows for development.	Algorithms are implemented in different programming languages; no response capabilities.
Jgraph	http://www.jgraph.com /mxgraph.html	Generate and manipulate graphs, assign attributes to links and nodes, has R and Python interfaces support for visualization, is open source.	Must be familiar with programming languages C, R, and Python; no response capabilities.
JUNG	https://blogs.reucon.com/asterisk-java/tag/visualization/	Create custom layouts and can annotate graphs, links, nodes with any Java data type.	Must be familiar with coding in Java to call the routines; no monitoring or response capabilities.
Visualization Library	http://visualizationlibrary.org/documentation /pag_gallery.html	Lightweight C++ OpenGL middleware, volume rendering, animation, and memory management.	Few analysis capabilities; no monitoring or response capabilities.
Igraph	http://igraph.sourceforge.net/screenshots.html	Generate and manipulate graphs; R package and Python module for 3-D interactivity; well documented for users and developers.	May only implement your own algorithms in C, R, Python or Ruby; one analysis capability; no monitoring nor response capabilities.
GINY	http://csbi.sourceforge.net/screenshots.html	An interface layer that is useful for building graphing projects.	Provides no official algorithms; few analysis capabilities; no response capabilities.

5.5 Graphical Data Representation Tools

Graphical data representation tools are designed to reveal patterns in the data that are difficult to detect otherwise. The visual depictions of data are almost universally understood without requiring knowledge of language. The visualization and graphical data representation tools accounted for in this survey includes AVS Express, Axiis, Cytoscape, Gephi, GGobi, GUESS, Inflow 3.1, LANet-Vi, NAViGaTOR, NodeXL, Pajek, Protovis, Tableau Desktop, and TouchGraph. They make up 14/59=23.7% of the total visualization tools surveyed for network analysts' tasks. Table 7 highlights the strengths and weaknesses of each visualization tool in this group.

Table 7. Graphical data representation tools' capabilities.

Graphical Data Representation Tools' Capabilities			
Name	**Web Sites (accessed 01/29/2014)**	**Strengths**	**Weaknesses**
AVS Express	http://www.cybernet.co.jp/avs/english/avsexpress.html	Uses hardware power, manages memory better, faster graphics, specialized modules, and cross-platforms.	Ease-of-use is medium to difficult; few analysis capabilities; no response capabilities.
Axiis	http://datavisualization.ch/showcases/visualizing-historic-browser-statistics-with-axiis/	Prebuilt visualization components, abstract layout patterns, rendering classes allow you to create your own visualizations.	No monitoring or response capabilities.
Cytoscape	http://nemo-cyclone.sourceforge.net/graphs.php	Domain-independent; calculate statistics of network, find shortest path, find clusters; integrates with (Igraph, Pajek, GraphViz, and more).	No analysis or response capabilities.
Gephi	https://gephi.org/	Exploratory data analysis, link analysis, social network analysis, biological network analysis, and poster creation.	No monitoring or response capabilities.
GGobi	http://www.statmethods.net/advgraphs/interactive.html	High dynamic and interactive graphics, R analysis, tour in high dimension, and display plug-in available.	No monitoring or response capabilities.
GUESS	http://graphexploration.cond.org/	Supports dynamic and time sensitive data; animation; import and export standard formats, works with other tools (JUNG, Prefuse, and TouchGraph).	No analysis capabilities.

Table 7. Graphical data representation tools' capabilities (continued).

Graphical Data Representation Tools' Capabilities			
Name	**Web Sites (accessed 01/29/2014)**	**Strengths**	**Weaknesses**
Inflow 3.1	http://www.orgnet.com/inflow3.html	Cluster analysis; network density; external and internal ratio; weighted average path length; shortest path; and path distribution.	No monitoring or response capabilities.
LANet-Vi	http://sourceforge.net/projects/lanet-vi/	Connectivity and clustering properties within a k-shell, and correlations between degree and shell index.	Programming language is C++; no monitoring or response capabilities.
NAViGaTOR	http://web.cs.toronto.edu/research/profiles/nav.htm	Queries OPHID/I2D online databases; displays networks in 2-D/3-D, provides analytical capabilities; supports standard input/output formats.	No monitoring or response capabilities.
NodeXL	http://www.connectedaction.net/nodexl/	Flexible import/export; direct connections to social networks, zoom scale; flexible layout; easily adjust appearance, dynamic filtering; powerful vertex grouping; graph metric calculations; and task automation.	No response capabilities.
Pajek	http://www.roget.org/graphics/pajekWXW.gif	Supports abstraction; implementation of sub-quadratic algorithms; clusters; extract and shrink vertices; multirelational networks; and 2mode networks.	No monitoring or response capabilities.
Tableau Desktop	http://www.tableausoftware.com/	Connect to data in file or on a server; handles spreadsheets, databases, and big data; more than 90 features; Web and mobile authoring; visual analytics; business integration; and high performance.	Not open source or free; only available on Windows and Mac platforms.
TouchGraph	http://scoutness.com/touchgraph-discover-the-relationships-contained-in-popular-information-sources/	Many relationship types supported; associate text and numerical attributes with nodes and edges; images can be associated with nodes; advanced clustering.	No response capabilities.

5.6 Innovative Visualization Tools

The innovative visualization tools are tools developed from projects, successful tools from other domain fields, and interesting research that can all be applied to the network security domain to aid analysts' tasks. The innovative tools accounted for in this survey includes Bloom Diagram, Circos, DocuBurst, NVIVO, PathFinder, PeopleGarden, SemaSpace, Schemaball, SocSciBot, The Web Stalker, ThinkMap, ThreadArcs, Visone, Visualyzer 2.1, and WebFan. They make up 15/59=25.4% of the total visualization tools surveyed for network analysts' tasks. Table 8 highlights the strengths and weaknesses of each visualization tool in this group.

Table 8. Innovative visualization tools' capabilities.

Innovative Visualization Tools' Capabilities			
Name	**Web Sites (all accessed 01/29/2014)**	**Strengths**	**Weaknesses**
Bloom Diagram	http://www.visualcomplexity.com/vc/project.cfm?id=358	Keyboard controls to zoom in, out, and pan around the screen; play animation over time.	No monitoring or response capabilities.
Circos	http://mkweb.bcgsc.ca/template/circos/$url_root/tableviewer/	Plaintext files are easily automated; simple format for input/output; rules are snippets of code.	No analysis or response capabilities.
DocuBurst	http://tapor.ca/?id=123	A radial, space-filling layout of hyponymy (IS-A relation); zoom; filter; document visualization.	Visualizes words only; no response capabilities.
NVIVO	http://blogs.city.ac.uk/educationalvignettes/2011/06/01/nvivo-software-training-for-support-qualitative-research-in-he/#.Ui8c7H-sYyY	Import YouTube videos; import social network posts; work with Web pages and online PDFs; work with non-English interfaces; and provide automatic coding for social networks.	More of a collaboration tool; no analysis, monitoring, or response capabilities.
PathFinder	http://tecfa.unige.ch/perso/yvan/PathFinder/	Displays the Web site structure and the customers navigation paths in a 3-D visualization.	Programming language is Java; not open source.
PeopleGarden	See reference 29 in the "References" list. http://dl.acm.org/citation.cfm?id=322581	Useful for threaded discussion space such as Usenet newsgroups and for interaction spaces like chat rooms.	No analysis or response capabilities.
SemaSpace	http://residence.aec.at/didi/FLweb/	Creates interactive graph layers in 2-D and 3-D; calculates complex networks; incorporate additional data such as images, sounds, and full texts.	No monitoring or response capabilities.

Table 8. Innovative visualization tools' capabilities (continued).

Innovative Visualization Tools' Capabilities			
Name	**Web Sites (all accessed 01/29/2014)**	**Strengths**	**Weaknesses**
Schemaball	http://mkweb.bcgsc.ca/schemaball/?tour	Creates flexible visualizations of database schemas; Schemas may be read from an SQL schema dump, flat file or live database.	No monitoring or response capabilities.
SocSciBot	http://webometrics.wlv.ac.uk/networkhelp/	Produces network diagrams for export to Pajek and UCINET and analyzes links.	One analysis capability; no response capability.
The Web Stalker	http://artsconnected.org/resource/89192/i-o-d-4-the-web-stalker	New refreshing visual metaphors of data for the Web.	Available by author only; no monitoring or response capabilities.
ThinkMap	http://www.thinkmap.com/thinkmapsdk.jsp	Interfaces are useful for communicating a dataset's structure; fully dynamic; deployed as a client only application.	Not open source or free; no analysis, monitoring, or response capabilities.
ThreadArcs	http://flowingdata.com/2008/03/19/21-ways-to-visualize-and-explore-your-email-inbox/	Provides chronology, relationships, stability, compactness, attribute highlighting, scaling, interpretation and meaning.	No analysis or response capabilities; unknown how to obtain software.
Visone	http://harambeenet.org/board07/apps/visone/visone-firststeps.html	Interactive GUI tailored for social networks; import and export of standard formats for social network data; and publication quality for exports.	No monitoring or analysis capabilities.
VisuaLyzer	http://socioworks.com/productsall/visualyzer/	Create graphs; import and export network data in many formats; Customize visual properties of node and link; Images of your choice can be used to represent nodes; Conduct analysis for calculating network and nodal level indices.	Only supports Windows; not open source or free; basic analysis; no monitoring or response capabilities.

Table 8. Innovative visualization tools' capabilities (continued).

Innovative Visualization Tools' Capabilities			
Name	**Web Sites (all accessed 01/29/2014)**	**Strengths**	**Weaknesses**
WebFan	http://www.visualcomplexity.com/vc/project_details.cfm?id=128&index=25&domain=social%20networks	Use of color, indicating user's page activities; accumulating user accesses over time to identify Web pages that are visited more often; allow direct navigation.	No response capabilities.

6. Survey Analysis

The visualization tools' capabilities were cross-referenced against the analysts' initial visualization needs highlighted at the beginning of this report. The initial visualization needs of the intended end user are categorized into a general cyber-analysis task phase model, which we have expanded from references 25. Our enhanced cyber analysis task phase model is now: Pre-Development (PD), Monitoring (M), Analysis (A), Response (R), and Future Development (FD). Within each particular task phase, the associated visualization needs have been numerically ordered following the task phase abbreviation (refer to table 9).

Table 9. Visualization needs for the pre-development phase.

Visualization Needs for the Pre-Development Phase	
PD1	Incorporate more effective and abstract concepts to visualize
PD2	Build "network of trust" into the visualization system
PD3	Incorporate a communication medium to share data
PD4	Integrate geo-location into environment
PD5	Incorporate human processing capabilities to analyze patterns and images

The "Visualization Needs for the Pre-Development Phase" chart (see table 9) has been coded for ease in readability in the bar graph (see figure 2) reflecting the actual number of tools that are capable of meeting that particular need in the Pre-Development Phase.

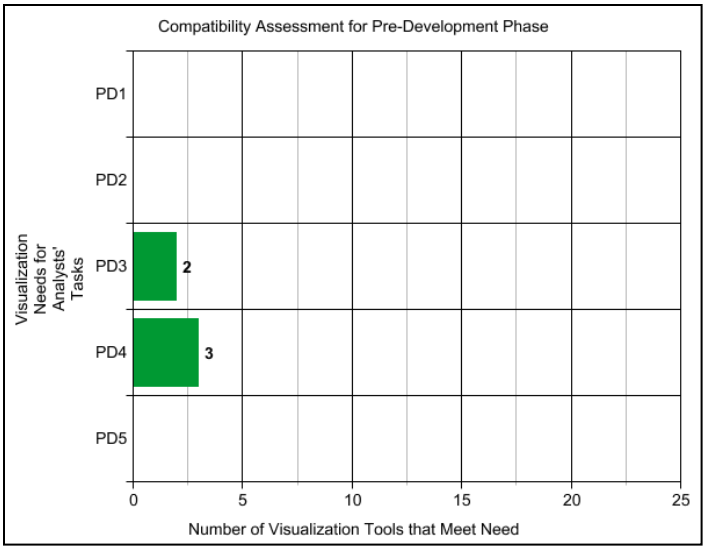

Figure 2. Visualization tools for the pre-development phase chart.

The overall applicability of the surveyed visualization tools that proved to meet the visualization needs for analysts' task in the Pre-Development Phase were six tools. Visualization need "PD3" may be accomplished by using visualization tools NVIVO or Impure. NVIVO allows import to YouTube videos, social network posts, and working collaboration with Web pages or online PDFs. Impure has preconfigured solutions accessible through multiple data sources. Both of these tools aid in incorporating a communication medium to share data to foster analysts' tasks.

Visualization need "PD4" may be accomplished by using visualization tools PlotPath, MapNet, and GeoPlot. PlotPath assigns x and y coordinates to nodes then arranges them horizontally. MapNet can view a network with or without the background map. GeoPlot plots a set of nodes and a set of lines that connects them to the user's location. These tools aid in the integration of geo-location into the display environment.

The "Visualization Needs for the Monitoring Phase" chart has been coded for ease in readability in the bar graph below reflecting the actual number of tools that are capable of meeting that particular need in the Monitoring Phase (refer to table 10 and figure 3).

Table 10. Visualization needs for the monitoring phase.

Visualization Needs for the Monitoring Phase	
M1	An overview of the alert data
M2	Simple displays
M3	Support for pattern and anomaly recognition
M4	Flexibility
M5	Speed of processing

Table 10. Visualization needs for the monitoring phase (continued).

Visualization Needs for the Monitoring Phase	
M6	Identify abnormalities
M7	Identify impacts of breaches
M8	Understand user perspective
M9	Use timeline to order events and actions

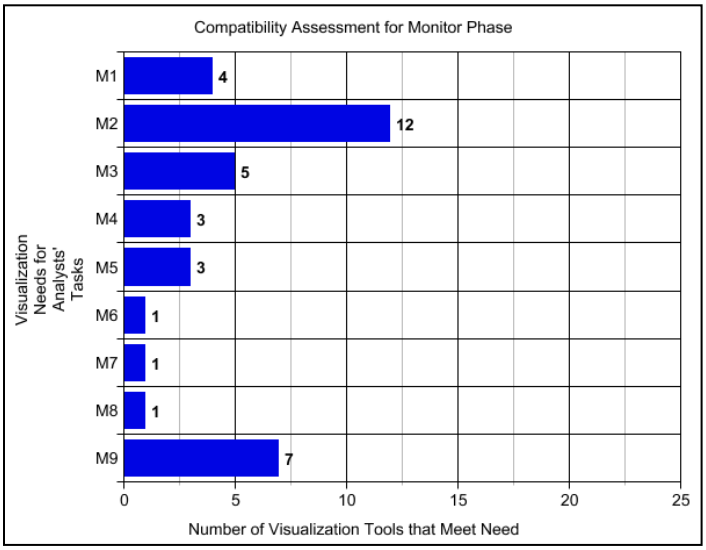

Figure 3. Visualization tools for the monitoring phase chart.

The overall applicability of the surveyed visualization tools that proved to meet the visualization needs for analysts' task in the Monitor Phase were thirty-three tools. Visualization need "M1" may be accomplished by using visualization tools AutoFocus, Cytoscape, Plankton, and SocSciBot. AutoFocus produces plots that can represent the entire network. Cytoscape calculates the statistics of a network, finds the shortest path, and clusters the data. Plankton does both topological and geographical displays of an entire network. SocSciBot produces standard statistics of interlinking network diagrams. These tools aid in giving the overview of alerts that may be present in a network.

Capability assessment for the following visualization need(s) for analysts' tasks:

- Visualization need "M2" may be accomplished by using visualization tools Circos, Cytoscape, DocuBurst, Impure, InfoVis CyberInfrastructure, Jgraph, NetDraw, Prefuse, Processing JS, Protovis, TouchGraph, and VTK. Circos Provides circular visualization only and no analysis capabilities. Cytoscape provides multiple simple layouts. DocuBurst provides a specific radial, space-filled layout of hyponymy (IS-A relation) layout for data. Impure has a rich library of interactive visualizations for data. InfoVis CyberInfrastructure

uses common layout algorithms for data representation. Jgraph has a selection of layouts including hierarchical layouts, organic layouts, and tree layouts. NetDraw has multiple options to represent data including direct manipulation and interactive styles. Prefuse provides various displays and layout components. Processing JS does animation, behaviors, layouts, and relationships. Protovis uses topological methods, math, shapes, structures, and rendering to produce various data representations. TouchGraph uses text and numerical attributes to associate with nodes and edges. VTK provides scalar, vector, tensor, texture, and volumetric methods. These tools aid in creating simple displays for analysts' tasks.

- Visualization need "M3" may be accomplished by using visualization tools Complex System SCILAB Toolbox, Cuttlefish, GINY, GraphViz, and Prefuse. Complex System SCILAB Toolbox measures degree distribution, averages neighboring degree, finds average clustering and shell index. Cuttlefish provides simple images, geographical maps, color-coded data, and animated GIF. GINY is an interface layer useful for building graphical objects. GraphViz makes available useful features for concrete diagrams and tabular node layout. Prefuse provides flexibility and animation support. These visualization tools have capabilities that when tweaked and placed in ensemble with other tools will support both pattern and anomaly recognition for analysts' tasks.
- Visualization need "M4" may be accomplished by using visualization tools GTrace, MapNet, and NodeXL. GTrace is flexible to support the addition of new databases. MapNet has flexibility in data representations. NodeXL is flexible with its layouts, import and output formats. These visualization tools are flexible in some aspect of capabilities presented to aid analysts' tasks.
- Visualization need "M5" may be accomplished by using visualization tools AVS Express, Otter, and Tableau Desktop. AVS Express manages memory better and provides faster graphics. Otter has high memory usage for large data sets. Tableau Desktop connects to data in a file or on a server with high performance rates. These visualization tools provide better speeds of processing compared to most visualization tools and this is a plus for aiding analysts' tasks.
- Visualization needs "M6" and "M7" may be accomplished by using visualization tool Walrus. Walrus does labeling and interactive pruning of graphs.
- Visualization need "M8" may be accomplished by using visualization tool PathFinder. PathFinder displays Web site structure and uses trace backs to understand user perspective. This capability may also be used to identify impacts of breaches and therefore aids the analysts' tasks.

- Visualization need “M9” may be accomplished by using visualization tools AutoFocus, Beluga, BloomDiagram, GUESS, RTG, Thread Arcs, and WebFan. AutoFocus has various time period layouts ranging from weeks to half-hour intervals. Beluga shows both total round trip time and per-hop round trip time. BloomDiagram plays animation of the activity over time. GUESS supports dynamic and time sensitive data. RTG polls at sub-one-minute intervals. Thread Arcs provides chronology and relationships found in e-mail. WebFan accumulates user accesses over time. These visualization tools use forms of timelines to order events and actions that aid analysts’ tasks.

The “Visualization Needs for the Analysis Phase” chart has been coded for ease in readability in the bar graph below reflecting the actual number of tools that are capable of meeting that particular need in the Analysis Phase (refer to table 11 and figure 4).

Table 11. Visualization needs for the analysis phase.

Visualization Needs for the Analysis Phase	
A1	Multiple views, zoom, drill down, focus+ context solutions
A2	Correlation between displays and linked views
A3	Filtering and data selection
A4	Have a clear focus on either mission impact or system impact
A5	Visualize characterization of attacks and attacker
A6	Visualize identity of legitimate user
A7	Switch between viewer perspectives to address what is interesting to look at
A8	Provide multidimensions beyond 2-D
A9	Usage of templates
A10	Representation that includes all nodes and routers
A11	Representation of a particular timeline of events
A12	Representation for generalized attack path

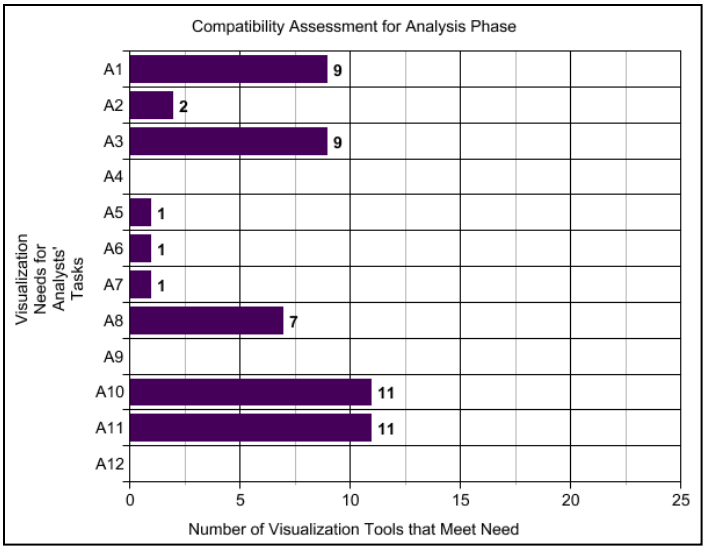

Figure 4. Visualization tools for the analysis phase chart.

The overall applicability of the surveyed visualization tools proved to meet the visualization needs for analysts' task in the Analysis Phase were thirty-seven tools. Visualization need "A1" may be accomplished by using visualization tools AutoFocus, BloomDiagram, Cichild, DocuBurst, Inflow 3.1, MapNet, NodeXL, Plankton, and Walrus. AutoFocus can drill down into separate pages for each category. BloomDiagram zooms in and out of network and pans around the screen. Cichild provides a zooming point of view. DocuBurst provides zooming and filter techniques. Inflow 3.1 allows internal and external ratio, weighted average path length, shortest path, and path distribution. MapNet views networks with or without background map. NodeXL has zoom scale and easily adjusts data appearance. Plankton provides display toggle, zoom, pan, and does time sequence animation. Walrus allows panning and zooming of network graphs. These visualization tools aid in providing multiple views, zoom, drill down, focus+ context solutions for analysts' tasks.

Capability assessment for the following visualization need(s) for analysts' tasks:

- Visualization need "A2" may be accomplished by using visualization tools Beluga and Bloom Diagram. Beluga provides statistical breakdown of Round Trip Times (RTTs) for trend analysis. Both visualization tools aid in providing correlation between displays and linked views for analysts' tasks.
- Visualization need "A3" may be accomplished by using visualization tools FlowScan, Impure, JUNG, NodeXL, Pajek, PlotPaths, Sci² Tool, The Web Stalker, and WebFan. FlowScan examines flow data and maintains counters. Impure accesses multiple data sources. JUNG provides filtering mechanisms. NodeXL provides dynamic filtering and powerful vertex grouping. Pajek extracts vertices, shrinks vertices, and finds clusters in networks. PlotPaths assigns x and y coordinates to nodes then arranges them. Sci² Tool does preprocessing, visualization, modeling, network extraction, and analysis. The Web

Stalker reads and manipulates information. WebFan allows direct navigation through network data. These visualization tools aid in providing filtering and data selection for analysts' tasks.

- Visualization needs "A5"and "A6" may be accomplished by using visualization tool GTrace. GTrace uses methods to either determine or guess at the physical location of a node in trace route path. This capability may be used to visualize characterization of attacks, attacker, and identity of legitimate user for analysts' tasks.
- Visualization need "A7" may be accomplished by using visualization tool Igraph. Igraph creates and manipulates directed and undirected graphs. This capability allows for easy switching between perspective views. It addresses what is interesting to look at for analysts' tasks.
- Visualization need "A8" may be accomplished by using visualization tools Cichild, GGobi, NAViGaTOR, PathFinder, SemaSpace, Visualization Library, and VTK. Cichild provides 3-D representation layouts. GGobi allows touring in high dimension. NAViGaTOR displays networks in 2-D and 3-D. PathFinder shows customers navigation paths in 3-D visualization. SemaSpace creates interactive graph layers in 2-D and 3-D. Visualization library has high performance 2-D and 3-D graphic applications. VTK creates 3-D graphics. These visualization tools provide capabilities for multiple dimensions beyond 2-D aiding analysts' tasks.
- Visualization needs "A10"and "A11" may be accomplished by using visualization tools Axiis, Cichild, GeoPlot, GGobi, GINY, Jgraph, LANET-Vi, NetDraw, Processing JS, Protovis, and TouchGraph. Axiis provides visualization components, abstract layouts, and create unique visualizations. Cichild does animation of bar charts, vertex, and edge graphs. GeoPlot plots a set of nodes and a set of lines that connects to an image specified by the user. GGobi provides high dynamic and interactive graphics. GINY an interface layer is useful for building graphical objects. Jgraph has a selection of layouts including hierarchical layouts, organic layouts, and tree layouts. NetDraw has multiple options to represent data including direct manipulation and interactive styles. Processing JS does topology, math, shapes, structures, and rendering. Protovis does animation, behaviors, layouts, and relationships. TouchGraph uses text and numerical attributes to associate with nodes and edges. These visualization tools provide representations for nodes, routers, and particular timeline of events for analysts' tasks.

The "Visualization Needs for the Response Phase" chart has been coded for ease in readability in the bar graph below reflecting the actual number of tools that are capable of meeting that particular need in the Response Phase (refer to table 12 and figure 5).

Table 12. Visualization needs for the response phase.

Visualization Needs for the Response Phase	
R1	Suggestion for response action
R2	Incident reporting
R3	Annotation/feedback to facilitate future analysis
R4	Saving views
R5	Historical display
R6	Reporting data transfer
R7	Visualize identified attacks and attackers
R8	Visualize malicious actor
R9	Visualize compromised systems
R10	Visualize an intended attack through trace back

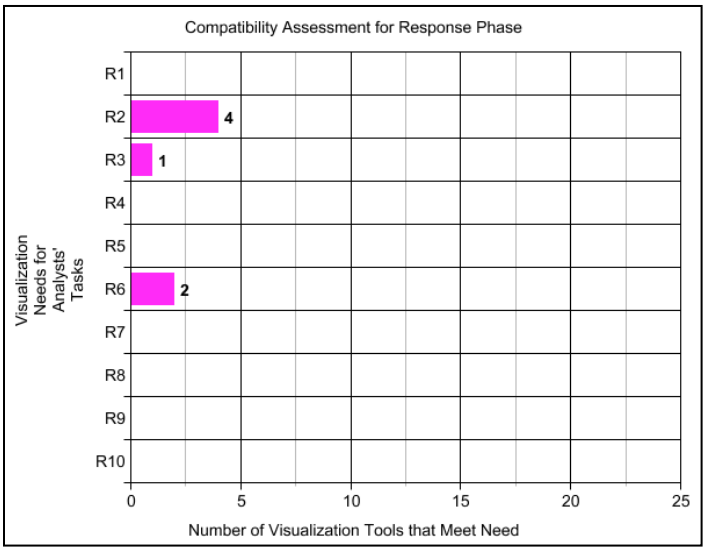

Figure 5. Visualization tools for the response phase chart.

The overall applicability of the surveyed visualization tools proved to meet the visualization needs for analysts' task in the Response Phase were seven tools. Visualization need "R2" may be accomplished by using visualization tools AutoFocus, FlowScan, Sci² Tool, and Visone. AutoFocus produces reports. FlowScan does analyses and produces reports for NetFlow format data. Sci² Tool provides database functionality, has a scheduler and does preparation. Visone has a nice publication quality for exports and is good for reporting. These tools aid in providing capabilities to make incident reporting more effective for analysts' tasks.

Capability assessment for the following visualization need(s) for analysts" tasks:

- Visualization need "R3" may be accomplished by using ClojureAtlas. This tool can access documentation, provide sources, and view relationships visually. ClojureAtlas is a good visualization tool in that its capabilities aid in documenting and reporting an attack.
- Visualization need "R6" may be accomplished by using GUESS, and FlowScan. GUESS imports and exports standard formats usable for reporting and data transfer. FlowScan analyzes and reports on NetFlow format data. Both of these tools make reporting data transfer simpler and possible.

The "Visualization Needs for the Future Development Phase" chart has been coded for ease in readability in the bar graph below reflecting the actual number of tools that are capable of meeting that particular need in the Future Development Phase (refer to table 13 and figure 6).

Table 13. Visualization needs for the future development phase.

Visualization Needs for the Future Development Phase	
FD1	Allow others to view current attacks
FD2	Integrate real-time (dynamic) animation
FD3	Connect global resources visually
FD4	Increase collaboration capabilities
FD5	Incorporate data and report sharing on various networks

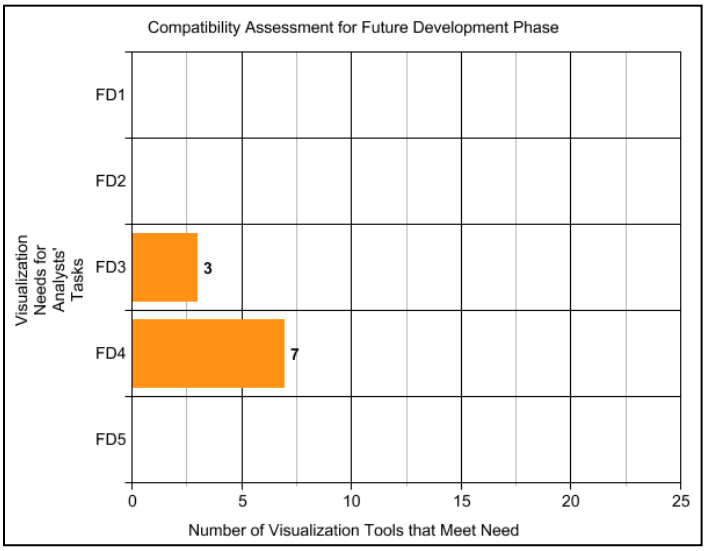

Figure 6. Visualization tools for the future development phase chart.

The overall applicability of the surveyed visualization tools that proved to meet the visualization needs for analysts' task in the Future Development Phase were seven tools. Visualization need "FD3" may be accomplished by using visualization tools GUESS, NVIVO, and Visone. GUESS works with other systems such as JUNG, Prefuse, and TouchGraph. NVIVO allows import to YouTube videos, social network posts, and working collaboration with Web pages or online PDFs. Visone does import and export of standard file formats for social network data and this capability can be applied to the network security domain. These tools aid in sharing resources to foster global data transmission for analysts' tasks.

Capability assessment for the following visualization need(s) for analysts' tasks:

- Visualization need "FD4" may be accomplished by using visualization tools GUESS, NVIVO, Visone, PeopleGarden, SemaSpace, SocSciBot, and ThinkMap. PeopleGarden is useful for threaded discussion spaces but needs to be incorporated into a communication medium. SemaSpace can incorporate additional data such as images, sounds, and full texts into a communication medium. SocSciBot exports network diagrams to Pajek and UCINET. This capability can be tweaked to extend to more databases and global resources. ThinkMap's data-driven technology for Web applications may be incorporated into a communication medium for ease of access to data. These tools aid in providing an environment for global collaboration and effective reporting.

In summary, out of the forty-one visualization needs, the surveyed visualization tools met twenty-five of them and sixteen of them were unmet. See figure 7.

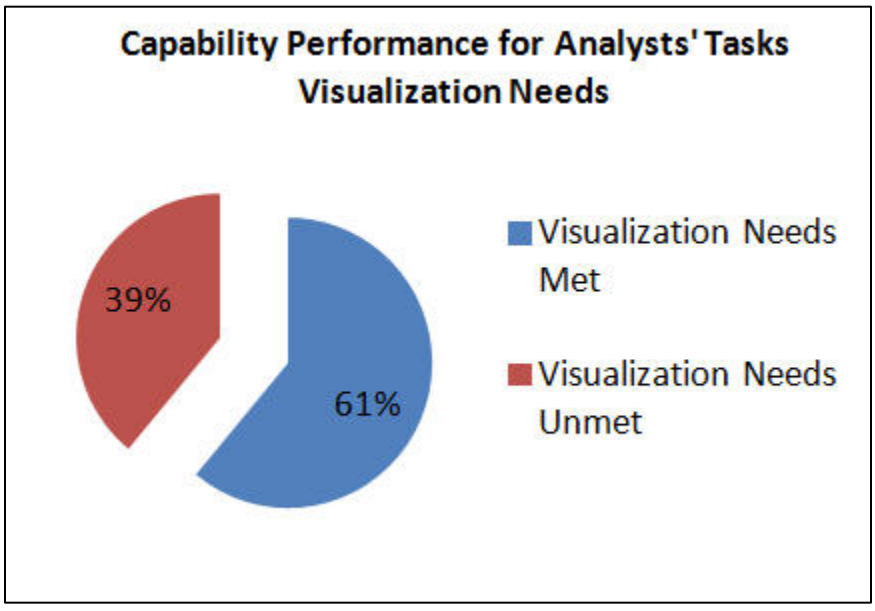

Figure 7. Visualization tools' overall capability performance meeting analysts' needs.

7. Conclusions

In this report, we evaluated which capabilities of existing visualization tools truly meet analysts' needs. Of the fifty-nine visualization tools, grouped as CAIDA tools, Visual Programming Language tools, Visual software Packages and Kits, Visualization Library tools, Graphical Data Representation tools, and Innovative Visualization tools proved that 61% of the visualization needs for analysts' tasks could be met. Surprisingly, 39% of the visualization needs for analysts' tasks remain unmet. Our findings demonstrate an immediate need for the development of visualization tools that can address the remaining visualization needs. This assessment pinpoints the need for improved user interfaces or environments for analysts who perform network security tasks. The survey's findings enable knowledge superiority over the malicious attackers for the entire network security community. This survey can be used to promote future work in testing and confirming that the identified 61% of surveyed visualization tools truly meet visualization needs for analysts' tasks. This assessment also drives ideas for innovative development and integration with other techniques in ensemble to aid IDS with analysts' tasks.

8. References

1. Debar, H.; Becker, M.; Siboni, D. A Neural Network Component for An Intrusion Detection System. In *Proceedings of the 1992 IEEE Computer Society Symposium on Research in Security and Privacy*, pages 240–250, Oakland, CA, May 1992.

2. Jagannathan, R.; Lunt, Teresa; Anderson, Debra; Dodd, Chris; Gilham, Fred; Jalali, Caveh; Javitz, Hal; Neumann, Peter; Tamaru, Ann; Valdes, Alfonso. *System Design Document: Next-Generation Intrusion Detection Expert System (NIDES)*; Technical Report A007/A008/A009/A011/A012/A014; SRI International, 333 Ravenswood Avenue, Menlo Park, CA 94025, March 1993.

3. Kumar, S.; Spafford, E. H. A Pattern Matching Model for Misuse Intrusion Detection. In *Proceedings of the 17th National Computer Security Conference*, pages 11–21, October 1994.

4. Spirakis, P.; Katsikas, S.; Gritzalis, D.; Allegre, F.; Darzentas, J.; Gigante, C.; Karagiannis, D.; Kess, P.; Putkonen, H.; Spyrou, T. SECURENET: A Network-Oriented Intelligent Intrusion Prevention and Detection System. *Network Security Journal* **November 1994**, *1* (1).

5. Axelsson, Stefan. *On a Difficulty of Intrusion Detection*; RAID, West Lafyette, IN, 1999.

6. Lunt, T. F.; Jagannathan, R.; Lee, R.; Listgarten, S.; Edwards, D. L.; Neumann, P. G.; Javitz, H. S.; Valdes, A. *IDES: The Enhanced Prototype A Real Time Intrusion Detection Expert System*; Technical Report SRI-CSL-88-12; SRI International, 333 Ravenswood Avenue, Menlo, CA, October 1988.

7. Snapp, S. R.; Brentano, J.; Dias, G. V.; Goan, T. L.; Heberlein, L. T.; Ho, C.; Levitt, K. N.; Mukherjee, B.; Smaha, S. E.; Grance, T.; Teal, Daniel M.; Mansur, D. DIDS (Distributed Intrusion Detection System) - Motivation, Architecture, and an Early Prototype. In *Proceedings of the 14th National Computer Security Conference*, pages 167–176, Washington, DC, October 1991.

8. Xu, K.; Zhang, Z.-L.; Bhattacharyya, S. Profiling Internet Backbone Traffic: Behavior Models and Applications. *SIGCOMMComput. Commun. Rev.* **2005**, *35* (4), pp. 169–180.

9. Staniford-Chen, S.; Cheung, S.; Crawford, R.; Dilger, M.; Frank, J.; Hoagland, J.; Levitt, K.; Wee, C.; Yip, R.; Zerkle, D. GrIDS A Graph-Based Intrusion Detection System for Large Networks. In *Proceedings of the 19th National Information Systems Security Conference*, 1996.

10. Axelsson, S. *Intrusion Detection Systems: A Taxonomy and Survey*; Technical Report No 99-15, Department of Computer Engineering: Chalmers University of Technology, Göteborg, Sweden, 1999

11. Axelsson, S. *Research in Intrusion-Detection Systems: A Survey and Taxonomy*, Department of Computer Engineering: Chalmers University of Technology, Göteborg, Sweden, 2000.

12. Denning, P. J. ACM President's Letter: What is Experimental Computer Science? *Commun. ACM* **1980**, *23* (10), 543–544.

13. McHugh, J.; Christie, A.; Allen, J. Defending Yourself: The Role of Intrusion Detection Systems. *Software, IEEE* **2000**, *17* (5), 42–51.

14. Department of Computer Science and Engineering; Chalmers-University of Gothenburg, SE-412 96 Goteborg, Sweden, December 1998. http://www.ce.chalmers.se/staff/sax (accessed 01/30/2014).

15. Monchi, O.; Petrides, M.; Petre, V.; Worsley, K.; Dagher, A. Distinct Neural Pathways Activated During Four Stages of the Wisconsin Card Sorting Task Using Event-Related Functional Magnetic Resonance Imaging. *Neuroimage* **2001**, *13* (6), S448–S448.

16. Ellis, G; Dix, A. An Explorative Analysis of User Evaluation Studies in Information Visualization. In *Proceedings of the 2006 AVI workshop on Beyond time and errors: novel evaluation methods for information visualization (BELIV '06)*, ACM, New York, NY, 1–7, 2006.

17. Erbacher, R. F.; Frincke, D. A.; Moody, S. J.; Fink, G. A Multi-Phase Network Situational Awareness Cognitive Task Analysis. *Information Visualization Journal* **2010**, 204–219.

18. Gerth, J. *Proceedings of the Seventh International Symposium on Visualization for Cyber Security*, ACM, New York, NY, 2010.

19. D'Amico, A.; Whitley, K. The Real Work of Computer Network Defense Analysts. *VizSEC 2007: Proceedings of the Workshop on Visualization for Computer Security*, Berlin, Heidelberg: Springer-Verlag, pp. 19–37, 2008.

20. Hiraishi, H.; Mizoguchi, F. Design of a Visual Browser for Network Intrusion Detection. In *Enabling Technologies: Infrastructure for Collaborative Enterprises, 2001. WET ICE 2001. Proceedings. Tenth IEEE International Workshops on* (pp. 132–137), IEEE, 2001.

21. Becker, R. A.; Eick, S. G.; Wilks, A. R. Visualizing Network Data. *Visualization and Computer Graphics, IEEE Transactions on* **1995**, *1* (1), 16–28.

22. Abdullah, K.; Lee, C.; Conti, G.; Copeland, J. A. Visualizing Network Data for Intrusion Detection. In *Information Assurance Workshop, 2005. IAW'05. Proceedings from the Sixth Annual IEEE SMC* (pp. 100–108), IEEE, June 2005.

23. Xin, J.; Dickerson, J. E.; Dickerson, J. A. Fuzzy Feature Extraction and Visualization for Intrusion Detection. In *Fuzzy Systems, 2003. FUZZ'03. The 12th IEEE International Conference on* (Vol. 2, pp. 1249–1254), IEEE, May 2003.

24. Erbacher, R. F.; Frincke, D. A.; Moody, S. J.; Fink, G. A Multi-Phase Network Situational Awareness Cognitive Task Analysis. *Information Visualization Journal* **2010**, 204–219.

25. Komlodi, A.; Goodall, J. R.; Lutters, W. G. An Information Visualization Framework for Intrusion Detection. In *CHI'04 extended abstracts on Human factors in computing systems* (p. 1743). ACM, April 2004.
26. CAIDA Tools–Overview of CAIDA Software Tools, http://www.caida.org/tools/ (accessed 01/30/2014).
27. Gates, C.; Collins, M.; Duggan, M.; Kompanek, A.; Thomas, M. More Netflow Tools for Performance and Security. In *Proceedings of the 18th USENIX conference on System administration* (pp. 121–132). USENIX Association, November 2004.
28. Johnston, W. M.; Hanna, J.R.P.; Millar, R. J. Advances in Dataflow Programming Languages (PDF). *ACM Computing Surveys* **2004**, *36* (1), 1–34. doi:10.1145/1013208.1013209. Retrieved 2011-02-16.
29. Xiong, R.; Donath, J. PeopleGarden: Creating Data Portraits for Users. *Proceedings of the 12th annual ACM symposium on User interface software and technology*. ACM, 1999.

Bibliography

Alpert, C. J.; Kahng, A. B. Recent Developments in Netlist Partitioning: A Survey. *Integration: The VLSI J.* **1995**, *19*, 1–81.

Andrews, K. Visualizing Cyberspace: Information Visualization in the Harmony Internet Browser. *Proc. IEEE Symp. Information Visualization (InfoViz '95)*, pp. 97–105, 1995.

Argawal, P. K.; Aronov, B.; Pach, J.; Pollack, R.; Sharir, M. Quasi-Planar Graphs Have a Linear Number of Edges. *Proc. Symp. Graph Drawing, GD '95*, pp. 1–7, 1995.

Becker, R. A.; Eick, S. G.; Wilks, A. R. Visualizing Network Data. *IEEE Trans. Visualization and Computer Graphics* **1995**, *1* (1), 16–28.

Ben-Shaul, I.; Herscovici, M.; Jacovi, M.; Maarek, Y. S.; Pelleg, D.; Shtalhaim, M.; Soroka, V.; Ur, S. Adding Support for Dynamic and Focused Search with Fetuccino. *Proc. Eighth Int'l World Wide Web Conf.*, 575–587, 1999.

Berry, J.; Dean, N.; Goldberg, M.; Shannon, G.; Skiena, S. Graph Drawing and Manipulation with LINK. *Proc. Symp. Graph Drawing GD '97*, 425–437, 1999.

Bertault, F. A Force-Directed Algorithm that Preserves Edge Crossing Properties. *Proc. Symp. Graph Drawing, GD '99*, 351–358, 1999.

Blythe, J.; McGrah, C.; Krackhardt, D. The Effect of Graph Layout on Inference from Social Network Data. *Proc. Symp. Graph Drawing, GD '95*, 40–51, 1995.

Botafogo, R. A.; Rivlin, E.; Schneiderman, B. Structural Analysis of Hypertexts: Identifying Hierarchies and Useful Metrics. *ACM Trans. Information Systems* **1992**, *10* (2).

Brandenburg, F. J.; Himsolt, M.; Rohrer, C. An Experimental Comparison of Force-Directed and Randomized Graph Drawing Algorithms. *Proc. Symp. Graph Drawing GD '95*, 1996.

Brandes, U.; Shubina, G.; Tamassia, R. Improving Angular Resolution in Visualizations of Geographic Networks. *Data Visualization '2000, Proc. Joint Eurographics and IEEE TCVG Symp. Visualization*, to appear.

Brandes, U.; Wagner, D. A Bayesian Paradigm for Dynamic Graph Layout. *Proc. Symp. Graph Drawing GD '97*, 236–247, 1997.

Card, S. K.; Robertson, G. G.; York, W. The WebBook and the Web Forager: An Information Workspace for the World Wide Web. *Human Factors in Computer Systems, CHI '96 Conf. Proc.*, pp. 111–117, 1996.

Carpendale, M.S.T.; Cowperthwaite, D. J.; Fracchia, F. D. 3D Pliable Surfaces. *Proc. UIST '95 Symp.*, pp. 217–266, 1995.

Carpendale, M.S.T.; Cowperthwaite, D. J.; Fracchia, F. D. Extending Distortion Viewing from 2D to 3D. *IEEE Computer Graphics and Applications* **1997**, *17* (4), 42–51.

Carpendale, M.S.T.; Cowperthwaite, D. J.; Fracchica, F. D.; Shermer, T. Graph Folding: Extending Detail and Context Viewing into a Tool for Subgraph Comparisons. *Proc. Symp. Graph Drawing GD '95*, pp. 127–139, 1996.

CarrieÁre, J.; Kazman, R. Research Report: Interacting with Huge Hierarchies: Beyond Cone Trees. *Proc. IEEE Conf. Information Visualization '95*, pp. 74–81, 1995.

Centos, http://www.centos.org/docs/4/html/rhel-sg-en-4/s1-ids-net.html, (accessed 01/30/2014).

Cesar, C. L. Graph Foundation Classes for Java. IBM, http://www.alphaWorks.ibm.com/tech/gfc, 1999 (accessed 01/30/2014).

Chen, C.; Carr, L. Visualizing the Evolution of a Subject Domain: A Case Study. *Proc. IEEE Visualization '99 Conf.*, pp. 449–452, 1999.

Chuah, M. C. Dynamic Aggregation with Circular Visual Designs. *Proc. IEEE Symp. Information Visualization (InfoViz '98)*, pp. 30–37, 1998.

Chuah, M. C.; Roth, S. F.; Mattis, J.; Kolojejchick, J. SDM: Malleable Information Graphics. *Proc. IEEE Symp. Information Visualization*, pp. 36–42, 1995.

Coxeter, H.S.M. *Introduction to Geometry*; John Wiley & Sons, Inc., 1973.

Cruz, I. F.; Tamassia, R. Online Tutorial on Graph Drawing (year not provided). http://cs.brown.edu/~rt/papers/gd-tutorial/gd-constraints.pdf (accessed 01/30/14).

Cruz, I. F.; Twarog, J. P. 3D Graph Drawing with Simulated Annealing. *Proc. Symp. Graph Drawing GD '95*, pp. 162–165, 1995.

Davidson, R.; Harel, D. Drawing Graphs Nicely Using Simulated Annealing. *ACM Trans. Graphics* **1996**, *15* (4), 301–331.

Debar, H. *An Introduction to Intrusion-Detection Systems*. IBM Research, Zurich Research Laboratory: Ruschlikon, Switzerland, pages 1–6, 2002.

Debar, H.; Dacier, M.; Nassehi, M.; Wespi, A. Fixed vs. Variable-Length Patterns for Detecting Suspicious Process Behavior. In *5th European Symposium on Research in Computer Security Computer Security (ESORICS 98)*, J-J Quisquater, Y. Deswarte, C. Meadows, and D gollmann Eds., volume 1485 of LNCS, pages 1–15, Louvain-la-Neuve, Belgium, September 1998, Springer-Verlag.

Debar, H.; Dacier, M.; Wespi, A. Reference Audit Information Generation for Intrusion Detection Systems. In *Information Systems Security, Proceedings of the 14th International Information Security Conference IFIP SEC'98*, R. Posch and G Papp, Eds., pages 405–417, Vienna, Austria and Budapest, Hungary, August 31–September 4, 1998 http://www.centos.org/docs/4/html/rhel-sg-en-4/s1-ids-net.html (accessed 01/30/2014).

Debar, H.; Dacier, M.; Wespi, A. Towards A Taxonomy of Intrusion Detection Systems. *Computer Networks* **April 1999**, *31* (8), 805–822.

Dengler, E.; Cowan, W. Human Perception of Laid-Out Graphs. *Proc. Symp. Graph Drawing GD '98*, pp. 441–444, 1998.

Denise, A.; Vasconcellos, M.; Welsh, D.J.A. The Random Planar Graph. *Congressus Numerantium* **1996**, *113*, 61–79.

di Battista, G.; Eades, P.; Tamassia, R.; Tollis, I. G. Algorithms for Drawing Graphs: An Annotated Bibliography. *Computational Geometry: Theory and Applications* **1994**, *4* (5), 235–282.

di Battista, G.; Eades, P.; Tamassia, R.; Tollis, I. G. *Graph Drawing: Algorithms for the Visualization of Graphs*; Prentice Hall, 1999.

Duncan, C. A.; Goodrich, M. T.; Kobourov, S. G. Balanced Aspect Trees and Their Use for Drawing Very Large Graphs. *Proc. Symp. Graph Drawing GD '98*, pp. 111–124, 1998.

Durand, D.; Kahn, P. MAPA. *Proc. Ninth ACM Conf. Hypertext and Hypermedia (Hypertext '98)*, 1998.

Eades, P. A Heuristic for Graph Drawing. *Congressus Numerantium* **1984**, *42*, 149–160.

Eades, P.; Feng, Q.-W. Multilevel Visualization of Clustered Graphs. *Proc. Symp. Graph Drawing GD '96*, pp. 101–112, 1997.

Eades, P.; Houle, M. E.; Webber, R. Finding the Best Viewpoints for Three-Dimensional Graph Drawings. *Proc. Symp. Graph Drawing GD '97*, pp. 87–98, 1998.

Eades, P.; Sugiyama, K. How to Draw a Directed Graph. *J. Information Processing* **1990**, *13* (4), 424–434.

Eick, S. G. A Visualization Tool for Y2K. *Computer* **1998**, *31* (10), 63–69.

Eklund, J.; Sawers, J.; Zeiliger, R. NESTOR Navigator: A Tool for the Collaborative Construction of Knowledge through Constructive Navigation. *Proc. Ausweb '99, Fifth Australian World Wide Web Conf.*, 1999.

Erbacher, R. F.; Forcht, K. A. Combining Visualization and Interaction for Scalable Detection of Anomalies in Network Data. *Journal of Computer Information Systems* **Summer 2010**, *50* (4), 117–126.

Everitt, B. *Cluster Analysis*, first ed. Heinemann Educational Books Ltd., 1974.

Fairchild, K. M. *Information Management Using Virtual Reality-Based Visualizations*; Virtual Reality: Application and Explorations, Academic Press, 1993.

Fairchild, K. M.; Poltrock, S. E.; Furnas, G. W. SemNet: Three-Dimensional Representation of Large Knowledge Bases. *Cognitive Science and Its Applications for Human-Computer Interaction*, Lawrence Erlbaum Assoc., 1988, pp. 201–233.

Formella, A.; Keller, J. Generalized Fisheye Views of Graphs. *Proc. Symp. Graph Drawing GD '95*, pp. 242–253, 1995.

Forster, M.; Pick, A.; Raitner, M. *Graph Template Library*, University of Passau, Germany. http://www.fim.uni-passau.de/en/fim/faculty/chairs/theoretische-informatik/projects.html(accessed 01/30/2014).

FreÂcon, E.; Smith, G. WebPathDA Three Dimensional Web History. *Proc. IEEE Symp. on Information Visualization (InfoViz '98)*, Washington, DC, 1998.

Frick, A.; Ludwig, A.; Mehldau, H. A Fast Adaptive Layout Algorithm for Undirected Graphs. *Proc. Symp. Graph Drawing GD '93*, pp. 389–403, 1994.

Fröhlich, M.; Werner, M. Demonstration of the Interactive Graph Visualization System da Vinci. *Proc. DIMACS Workshop Graph Drawing '94*, 1995.

Fruchterman, T.M.J.; Reingold, E. M. Graph Drawing by Force-Directed Placement. *SoftwareDPractice & Experience* **1991**, *21*, 1,129–1,164.

Furnas, G. W. Generalized Fisheye Views. *Human Factors in Computing Systems, CHI '86 Conf. Proc.*, pp. 16–23, 1986.

Source http://source.mozillaopennews.org/en-US/articles/conversation-data-viz-experts/ (accessed 01/30/14).

KDD Cup 1999 Data http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html (accessed 01/30/2014).

McHugh, J. The 1998 Lincoln Laboratory IDS Evaluation. in *Proc. 3rd Int. Workshop Recent Adv. Intrusion Detection (RAID)*, Springer-Verlag: London, UK, 2000, pp. 145–161.

Misue, K.; Eades, P.; Lai, W.; Sugiyama, K. Layout Adjustment and the Mental Map. *J. Visual Languages and Computing* **1995**, *6*, 183–210.

Massachusetts Institute of Technology, Lincoln Laboratory; DARPA Intrusion Detection Evaluation, http://www.ll.mit.edu/mission/communications/ist/corpora/ideval/index.html (accessed 01/30/14).

Mukherjea, S.; Foley, J. D.; Hudson, S. Visualizing Complex Hypermedia Networks through Multiple Hierarchical Views. *Human Factors in Computing Systems, CHI '95 Conf. Proc.*, pp. 331–337, 1995.

Card, S. K.; MacKinlay, J. D.; Shneiderman, B. *Readings in Information Visualization*, Academic Press; A Harcourt Science and Technology Company; San Diego, CA, 1999.

Tan, K. M. C.; Killourhy, K. S.; Maxion, R. A. Undermining An Anomaly-Based Intrusion Detection System Using Common Exploits, *5th International Symposium on Recent Advances in Intrusion Detection (RAID)*; Zuirch, Switzerland, 2002.

Tavallaee, M.; Stakhanova, N.; Ghorbani, A. Toward Credible Evaluation of Anomaly-Based Intrusion-Detection Methods. *IEEE Trans. Syst., Man, Cybern. C, Appl. Rev* **Sep. 2010**, *40* (5), 516–524.

Walter, B.; Blecker, C.; Kirsch, P.; Sammer, G.; Schienle A.; Stark R.; Vaitl, D. MARINA: An Easy to Use Tool for the Creation of Masks for Region of Interest Analyses. In *9th International Conference on Functional Mapping of the Human Brain*, New York, NY, 2003.

Likert Scale, Wikipedia, http://en.wikipedia.org/wiki/Likert_scale (accessed 01/30/14).

List of Symbols, Abbreviations, and Acronyms

A	Analysis
AFL	Academic Free License
AFRL	United States Air Force Research Laboratory
ARL	U.S. Army Research Laboratory
CAIDA	Cooperative Association for Internet Data Analysis
DDoS	distributed denial-of-service
DIDS	Distributed IDS
DNS	Domain Name System
EPL	Eclipse Public License
FD	Future Development
fMRI	functional magnetic resonance imaging
GIF	Graphics Interchange Format
GrIDS	graph-based IDS
GUI	Graphical User Interface
HCI	human-computer interactions
ID	intrusion detection
IDS	Intrusion Detection System(s)
IP	Internet Protocol
M	Monitoring
PD	Pre-Development
PNNL	Pacific Northwest National Laboratory
R	Response
RTG	Real Traffic Grabber
RTT	Round Trip Time

TCP	Transmission Control Protocol
VizSec	Visualization Security
VPL	visual programming language
VTK	Visualization Toolkit
WCST	Wisconsin Card Sorting Task

NO. OF COPIES	ORGANIZATION
1 (PDF)	DEFENSE TECHNICAL INFORMATION CTR DTIC OCA
2 (PDF)	DIRECTOR US ARMY RSRCH LAB RDRL CIO LL IMAL HRA MAIL & RECORDS MGMT
1 (PDF)	GOVT PRINTG OFC A MALHOTRA
2 (PDF)	DIR USRL RDRL CIN D R E ETOTY R F ERBACHER

INTENTIONALLY LEFT BLANK.